

CLAIMS

What is claimed is:

- 1 1. An apparatus to manage a plurality of device configurations
2 comprising:
3 a control server to generate a job to update a device;
4 a control point to establish a secure communication with the control
5 server, and to receive the job;
6 the control point to establish communication with the device in
7 accordance with a maintenance schedule, and to update the device using the job.
- 1 2. The apparatus of claim 1, wherein the control server and the
2 control point are co-resident on a single computer system.
- 1 3. The apparatus of claim 1, wherein the control point is further to
2 communicate a result of the update process to the control server.
- 1 4. The apparatus of claim 3, wherein the communication of the result
2 of the update process comprises a transcript of communication between the
3 device and the control point.
- 1 5. The apparatus of claim 1, further comprising:
2 a data store coupled to the control server, the data store including a device
3 profile identifying the device to be updated and the device's characteristics.
- 1 6. The apparatus of claim 5, wherein the control server comprises:

2 a data generator to generate device specific data from the device profile;
3 and
4 a template interpreter to generate the job script based on the device
5 specific data and template data.

1 7. The apparatus of claim 6, wherein a template group is attached to
2 the device profile.

1 8. The apparatus of claim 6, wherein each device profile includes a
2 device type, and a template group is attached to each device type.

1 9. The apparatus of claim 6, wherein the template interpreter further
2 points to configuration files and supporting files.

1 10. The apparatus of claim 9, wherein the control point uses the job to
2 interact with the device, and uploads the configuration files to the device.

1 11. The apparatus of claim 1, wherein the job is to audit the device.

1 12. The apparatus of claim 11, wherein the audit comprises retrieving
2 configuration files from the device.

1 13. The apparatus of claim 11, wherein the audit comprises retrieving
2 firmware from the device.

1 14. The apparatus of claim 11, wherein the audit comprises obtaining a
2 checksum of the firmware of the device

1 15. The apparatus of claim 1, wherein the control server generates a job
2 in response to receiving a change in the device profile.

1 16. The apparatus of claim 15, wherein the change in the device profile
2 is made using a command line interface.

1 17. The apparatus of claim 1, wherein the control server further
2 comprises a control point generator to permit creation of a new control point.

1 18. The apparatus of claim 17, wherein the control point generator
2 comprises:
3 a localizer to generate a localized control point executable;
4 wherein the localization identifies a control server, such that the control
5 point executable may only interface with the identified control server.

1 19. The apparatus of claim 18, wherein the identified control server is a
2 control server group.

1 20. The apparatus of claim 19, wherein a single control server is
2 designated as a default control server, and other members of the control server
3 group enable fail-over if the default control server is unavailable.

21. The apparatus of claim 18, wherein the localized control point
executable includes the control server's public key.

1 22. The apparatus of claim 17, wherein the control point generator
2 comprises:
3 a pass phrase generator to generate a one-time pass phrase;
4 wherein upon installing a localized control point executable, the localized
5 control point executable is activated using the pass phrase.

1 23. The apparatus of claim 22, wherein the pass phrase is a series of
2 words from a dictionary.

1 24. The apparatus of claim 23, wherein pass phrase encodes a one-time
2 password.

1 25. The apparatus of claim 17, wherein when the new control point is
2 initialized using the localized control point executable, the new control point
3 comprises:
4 a key generation logic to generate a public key and a private key for the
5 control point;
6 a secure communication mechanism to communicate with the control
7 server using a one-time password encoded in a pass phrase used to generate the
8 new control point; and

9 the secure communication mechanism to complete a key exchange with
10 the control server, such that public key cryptography is used for further secure
11 communication.

1 26. The apparatus of claim 1, further comprising:
2 a scheduler in the control server to schedule an update of a particular
3 device coupled to a control point, and when it is time to update the particular
4 device, to send a communication request to the control point; and
5 a secure communication mechanism in the control point to respond to the
6 request by establishing a secure communication link with the control server.

1 27. The apparatus of claim 26, wherein the secure communication link
2 is secure shell (SSH).

1 28. The apparatus of claim 26, wherein the secure communication link
2 is secure sockets layer (SSL).

1 29. The apparatus of claim 26, wherein the time to schedule an update
2 of a particular device corresponds to a maintenance window of the device.

1 30. The apparatus of claim 26, wherein the device being updated is the
2 control point.

1 31. The apparatus of claim 1, wherein the control point further
2 comprises:

3 a scheduler to schedule execution of each job received by the control
4 point; and
5 a reporter to report back results of the execution of each job to the control
6 server.

1 32. The apparatus of claim 31, wherein the results comprise a complete
2 transcript of communication with the device to which the job was directed.

1 33. The apparatus of claim 1, further comprising a data store including
2 a device profile defining a current state of the device.

1 34. The apparatus of claim 33, wherein the data store is a SQL
2 database, and the data store is displayed as a hierarchical data store.

1 35. The apparatus of claim 33, wherein the data store comprises a
2 plurality of data types and new data types may be arbitrarily defined.

1 36. The apparatus of claim 33, wherein the data store further comprises
2 the past states of the device.

1 37. The apparatus of claim 34, further comprising a service module
2 coupled to the control server, the service module to define a functionality that
3 may be provided through the control server, the service module having a
4 separate user interface.

1 38. The apparatus of claim 37, wherein a service module comprises:
2 a user interface;
3 a command line interface to receive user input and convert it into
4 commands; and
5 a service module core to define a functionality to alter data in the data
6 store, such that the change flows down to the control points and the devices.

1 39. The apparatus of claim 38, wherein the service module core is
2 further to define arbitrary attributes for data in the data store.

1 40. A control server to manage a plurality of device configurations
2 comprising:
3 a data store to store current status of each device;
4 a user interface to alter data in the data store to prompt creation of a job;
5 a scheduler to schedule jobs to update devices;
6 a control point interface to send jobs to a control point, and to receive a
7 result from the control point.

1 41. The control server of claim 40, wherein the user interface is a
2 command line interface (CLI) permitting the creation of action scripts to make
3 complex alterations to the devices, the control points, and the data store.

1 42. The control server of claim 40, wherein the data store is an SQL
2 database presented in a hierarchical fashion.

1 43. The control server of claim 40, further comprising a device module
2 to generate a job for a particular device.

1 44. The control server of claim 43, wherein the device module
2 comprises:
3 a controller to create data from a device profile; and
4 a master to create a job using the data produced by the controller.

1 45. The control server of claim 44, wherein the master further to
2 determine whether to create a job.

1 46. The control server of claim 44, wherein the device module further
2 comprises:
3 a template to create device configuration files; and
4 a job to deliver changes to the device.

1 47. The control server of claim 44, wherein the device profile comprises
2 a descriptive triplet including a device module name, device platform, and
3 firmware revision, the device profile specifying how a particular device is
4 configured.

1 48. A control point to serve as an interface to a plurality of devices, the
2 control point managed by a control server, the control point comprising:
3 a scheduling logic to schedule a job in accordance with a maintenance
4 window defined by the job;

5 an execution environment for a delivery driver to deliver a job to a device
6 in accordance with the maintenance window of the device, as specified by the
7 job.

1 49. The control point of claim 48, further comprising:
2 the scheduling logic to schedule interfacing the control point with the
3 control server to receive jobs and updates.

1 50. The control point of claim 48, further comprising:
2 a secure communications channel to securely communicate with a control
3 server.

1 51. The control point of claim 48, wherein the control point is a stand-
2 alone system, running a secure/hardened operating system.

1 52. The control point of claim 48, wherein the control point operates as
2 an application on a non-dedicated computer system.

1 53. The control point of claim 52, wherein the control point on the non-
2 dedicated computer system further comprises:
3 a system state monitor to control the network and network applications
4 settings on the standard computer system.

1 54. The control point of claim 48 further comprising:

2 a cache to store files used by a job, such that the files may be reused and
3 the jobs sent need not include the files.

1 55. The control point of claim 54, a wherein a job includes references to
2 a plurality of files, and if the files are not in the cache, the secure communications
3 channel further to request the files from the control server.

1 56. The control point of claim 48, further comprising:
2 an execution environment for delivery drivers to execute the indicated
3 processes and jobs.

1 57. The control point of claim 48, wherein the control point has a
2 maintenance window, such that the control point is updateable by the control
3 server.

1 58. A method of controlling a network comprising:
2 determining if there is a job for a control point;
3 establishing a secure connection between a control server and the control
4 point;
5 sending the job to the control point, including a maintenance window
6 during which the job is to be performed; and
7 receiving job statuses of previous jobs from the control point; and
8 closing the connection with the control point.

1 59. The method of claim 58, wherein the job is to update the control
2 point, and the maintenance window is the maintenance window of the control
3 point.

1 60. The method of claim 58, wherein the job is to update a device
2 coupled to the control point.

1 61. The method of claim 58, wherein if the job is to update a device
2 coupled to the control point, the maintenance window is the maintenance
3 window of the device to which the job applies.

1 62. A method of controlling a network comprising:
2 establishing a secure session between a control server and a control point;
3 receiving a job from the control server, including a maintenance window
4 during which the job is to be performed;
5 putting the job into a job queue;
6 sending job statuses of previous jobs to the control server; and
7 closing the connection with the control server.

1 63. The method of claim 62, further comprising:
2 determining that there is a job in the job queue that has a current
3 maintenance window;
4 connecting to the device using credentials;
5 executing the job in the control point to affect the device;
6 storing the results of the job as the job status; and

7 disconnecting from the device.

1 64. The method of claim 63, wherein the credentials are a password.

1 65. The method of claim 63, wherein running the job comprises:
2 determining if the device is in an expected state; and
3 updating and configuring the device as specified by a job script within the
4 job.

1 66. The method of claim 63, wherein if the device is not in the expected
2 state, the device is not updated, and the non-compliant state data is returned to
3 the control server.

1 67. The method of claim 66, further comprising:
2 raising an alarm when the non-compliant state data is returned.

1 68. A method of controlling a network including a control point
2 controlled by a control server, the control point controlling the devices on the
3 network in accordance with jobs sent by the control server, the method including
4 creating new control points, the method of creating a control point comprising:
5 generating a branded executable for the control point including the
6 control server's public key;
7 generating a passphrase including a one-time password for activating the
8 control point; and

9 upon installation of the branded executable and activation with the
10 passphrase, receiving a connection from the new control point using the one-
11 time password from the passphrase.

1 69. The method of claim 68, further comprising:
2 verifying that the control point identified by the one-time password is
3 valid and not yet activated; and
4 establishing a secure communications channel with the control point.

1 70. The method of claim 68, wherein the passphrase is a plurality of
2 words in the English language.

1 71. The method of claim 68, wherein the passphrase is three or more
2 words having four or more letters, such that the passphrase is easily transmitted
3 via voice communication.

1 72. The method of claim 68, further comprising:
2 creating a public/private keypair for the new control point, and using that
3 public/private keypair for establishing secure communication with the control
4 point.

1 73. A method of controlling a network using a control server, the
2 method comprising:
3 maintaining a data store including configurations of each device coupled
4 to the control server through a control point;

5 generating a job to update a device;
6 receiving a report from the control point regarding the execution of the
7 job to update the device; and
8 storing in the data store the report with the current configuration of the
9 device, such that a complete revision history of the device is maintained.

1 74. The method of claim 73, wherein the revision history of the device
2 includes a previous device profile for that device, enabling a new device to be
3 configured identically to the original device, even if the new device is of a
4 different make.

1 75. The method of claim 73, wherein the revision history of the device
2 includes a previous device configuration file, enabling a review of the state of the
3 device at any point in the past.

1 76. The method of claim 73, wherein the revision history includes time
2 and date stamps for each alteration to a device.

1 77. The method of claim 73, wherein the job is generated in response to
2 a change in the data store.

1 78. A method of controlling a network including a control point
2 controlled by a control server, the control point interacting with the devices on
3 the network in accordance with jobs sent by the control server, the method
4 comprising generating a job comprising:

